[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
H04N 5/913

[12]发明专利申请公开说明书

[21]申请号 98811533.6

[43]公开日 2001 年 1 月 10 日

[11]公开号 CN 1279861A

[22]申请日 1998.9.22 [21]申请号 98811533.6
[30]优先权
[32]1997.9.25 [33]EP [31]97402238.6
[86]国际申请 PCT/IB98/01511 1998.9.22
[87]国际公布 WO99/16244 英 1999.4.1
[85]进入国家阶段日期 2000.5.25
[71]申请人 卡纳尔股份有限公司
地址 法国巴黎
[72]发明人 M·梅拉德

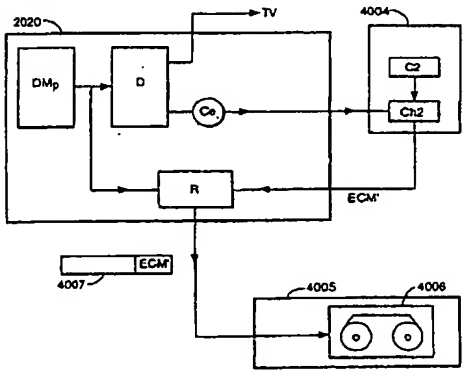
[74]专利代理机构 中国专利代理(香港)有限公司
代理人 吴立明 陈景峻

权利要求书 2 页 说明书 10 页 附图页数 6 页

[54]发明名称 记录加密数字数据的方法及装置

[57]摘要

一种用于传输及录制加密信息(Ce)的方法,其中该信息(Ce)是 用第一密钥加密并以加密形式传输的,加密信息(Ce)被拥有解密该信 息所必须的第一密钥的对等物的解码器(2020)接收,其特征在于用存 储在适合于被解码器(2020)与/或数字录象设备(4005)接纳的便携式支持设备(4004)中的第二密钥重新加密解密的信息(Ce),然后将 重新加密的信息录制在数字记录介质(4006)上。在重播录制品时,用 存储在支持装置(4004)中的第二密钥(C2)解密该信息。在特别好的 实施例中,信息(Ce)对应于用来扰频与解扰传输的数据的控制字,重 新加密的控制字(Ce)与仍然扰频的传输数据一起存储在记录介质 (4006)上。



ISSN1008-4274

权 利 要 求 书

1. 一种用于传输及录制加密数字信息的方法，其中数字信息是用第一密钥加密并以加密形式传输的，具有对解密该信息所必需的第一密钥的对等物的访问权的解码器接收加密的信息，及其特征在于此后用存储在适合于被该解码器或相关数字录象机接纳的便携式支持设备中的第二密钥重新加密该解密的信息，此后用该数字录象机将重新加密的信息录制在数字记录介质上。

2. 权利要求 1 中所要求的方法，其中该数字信息对应于用于解扰扰频的数字数据的控制字，扰频的数字数据是与该控制字一起用第一密钥加密传输的，此后该控制字用对等的第一密钥解密并用第二密钥重新加密，及然后将重新加密的控制字与扰频数据录制在数字记录介质上。

3. 权利要求 1 或 2 所要求的方法，其中该便携式支持设备为适合于被解码器与/或数字录象机中的智能卡阅读器接纳的智能卡。

4. 权利要求 3 中所要求的方法，其中该智能卡还包含用来解密用于初始解扰数据的控制字的第一密钥的对等物。

5. 权利要求 3 中所要求的方法，其中该第二密钥是存储在与解码器用来存储第一密钥的装置不同的智能卡上的。

6. 权利要求 3 至 5 中任何一项中所要求的方法，其中使用单一智能卡与第二密钥来为多个录制品生成重新加密的码字。

7. 权利要求 3 至 6 中任何一项中所要求的方法，其中该智能卡还包含若干信用单位来确定录制品可重播的次数，单位的数目是随着录制品的随后每一次部分或完整播放而递减的。

8. 权利要求 7 中所要求的方法，其中这些信用单位是与录制品的特定段关联的，使得播放一段录制品递减与该段关联的一定信用单位。

9. 权利要求 8 中所要求的方法，其中这些信用单位具有单一的类型并随着录制品的任何段的播放而递减。

10. 权利要求 1 中所要求的方法，其中该便携式支持是由记录介质本身定义的，第二密钥存储在嵌入该数字记录介质的外壳中的集成电路中。

11. 一种适用于传输及录制权利要求 1 至 10 中任何一项中所要求的扰频数字数据的装置，包括用于以第一密钥加密数字信息及以加密形式发射所述信息的发射机，用于接收加密的信息并具有对解密该信息所

必需的第一密钥的对等物的访问权的解码器，以及适合于被解码器或相关数字录象机接纳并拥有用于重新加密解密的信息供随后传输给数字录象设备供录制在数字记录介质上的第二密钥的便携式支持设备。

12．一种用于权利要求11的装置及适合于用在权利要求1至10中任何一项的方法的解码器，包括用于接纳拥有用于重新加密解密的信息的第二密钥的便携式支持设备的插槽。

13．权利要求12中所要求的解码器，与用于将重新加密的信息录制在数字记录介质上的数字录象设备集成。

说　明　书

记录加密数字数据的方法及装置

本发明涉及记录诸如电视广播等扰频数字数据的方法及装置。

加密数据传输是在收费电视系统领域中众所周知的，其中通常用卫星将扰频的音象信息广播给若干用户，各用户拥有能解扰传输的节目供以后观看的解码器或接收机/解码器。

在典型的系统中，扰频数字数据是与用于解扰该数字数据的控制字一起传输的，该控制字本身是用第一密钥加密并以加密方式传输的，拥有解密该加密的码字所必需的第一密钥的对等物的解码器接收扰频数字数据及加密的码字并随后解扰传输的数据，解码器适应于将仍在其扰频形式中的数字数据传递给数字记录设备。付费用户在逐月的基础上接收解密该加密的控制字所必需的密钥以便允许观看特殊节目。

随着数字技术的进展，传输的数据的质量已提高了许多倍。与数字质量数据相关的特殊问题在于其容易复制。当通过模拟链路（如，“Peritel”链路）传递解扰的节目供观看及用标准 VCR 录制时，质量保持不高于用标准模拟盒式带录制的相关质量。可将这一录制作为母带来进行盗版复制的危险性因而不大于标准的从商店购买的模拟盒式带。

作为对比，用直接数字链路传递给新一代的数字录制设备（例如 DVHS 录象机)之一的任何解扰的数字数据将具有与原始传输的节目相同的质量，并从而可复制任何次数而无任何图像或声音质量降低。因此存在着将解扰的数据用作母录制品来进行盗版复制，或者进一步的数字复制或甚至简单的模拟 VHS 复制，的很大危险性。

法国专利申请 9503859 示出利用永不允许将解扰的数字数据录制在数字记录介质上的系统来克服这一问题的一种方法。反之，该申请中所描述的解码器将在其扰频形式中的数据连同另一密钥重新加密的解扰数据所必需的控制字一起记录在记录介质上。这一新密钥只对接收机/解码器知道并替换所需的第一密钥来获取用于观见节目的码字。

这一系统的优点在于数据永不以“清晰”形式存储及在不拥有存储在接收机/解码器中的新密钥时不能观看。该系统还具有下述优点，由于在逐月的基础上改变第一密钥，使用不变的密钥来重新加密登记在数

字带上的控制字意味着接收机/解码器即使在定购的月份结束之后仍能解密记录在带上的控制字。

该专利申请中提出的系统的缺点在于只能结合该特定接收机/解码器观看。如果该解码器故障或被替换，便不再能播放该录制品。同样，不可能在不连接该系统中的接收机/解码器的数字录象机中直接播放录音品，因此观众必须保持与收费电视公司的订购，以便保有该解码器而才能观看已传输的影片。

本发明的目的为克服与这一解决方法关联的问题同时保持能保障数字数据录制品不能容易地用于生成传输的数据的盗版复制品。

本发明包括传输及录制加密数字信息的方法，其中数字信息是用第一密钥加密并以加密形式传输的，具有对解密该信息所必需的第一密钥的对等物的访问权的解码器接收加密的信息，其特征在于此后用存储在便携式支持设备中的适合于由解码器或相关数字录象机接收的第二密钥重新加密该解密的信息，以后数字录象机将重新加密的信息录制在数字记录介质上。

以这一方法，本发明克服了先有技术的问题，由于录制的数据的以后的重新播放成为独立于解码器本身。当重新播放录制品时，信息是用存储在支持装置上的第二密钥解密的。

只要新解码器具有接纳包含第二密钥的支持装置的插槽，替换解码器不会使所关心的录制品无效。如果提供有适当的阅读器，数字录象机本身可换取该第二密钥并允许重新播放信息而无须解码器。与容易故障的相对复杂的设备的解码器不同，该便携式支持设备可用简单的坚固形式实现。

用第二密钥重新加密及存储在数字记录介质上的信息可以简单地对应于音象信息。然而，在较佳实施例中，数字信息对应于用于解扰扰频的数字数据的控制字，扰频的数字数据是与作为用第一密钥加密的控制字一起传输的，然后用对等的第一密钥解密该控制字并用第二密钥重新加密，然后将重新加密的控制字与扰频数据录制在数字记录介质上。

在一个特别好的实施例中，该便携式支持设备为适合于解码器与/或数字录象机中的智能卡阅读器接受的智能卡。在本申请中，名词“智能卡”用于指称拥有诸如微处理器或用于储存第二密钥算法的 EEPROM 存储器等的任何常规的基于芯片的卡设备。同时包含在这一名词中的有

具有其它物理形式的芯片设备，例如在电视解码器系统中常用的钥匙形设备。

在一个实施例中，智能卡还包含用于解密控制字的第一密钥的对等物，用于诸如在电视广播系统的情况中为观看而初始解扰数据。在这一情况中，智能卡构成收费电视系统的一部分并且还可包含发射机知道的个人化密钥，使发射机能有选择地识别哪些用户在月底将接收更新的第一密钥。

在另一实施例中，第二密钥是存储在与用来存储第一密钥不同的智能卡上的。在这一实施例中，因而存储在数字介质上的信息的读取完全与用户系统分开，即使在用户已从系统退出并退出其订阅卡之后，只要他拥有的数字录象机/播放机适用于读取伴随的智能卡，他便能继续观看以前录制的电影。

在这一系统中，单一智能卡与第二密钥可用来为多个录象节目生成重新加密的码字。以这一方式，单一“信息库卡”可用来解密任何数目的录象节目。

在一个实施例中，智能卡还可包含若干信用单位来确定可以重播录象节目多少次，单位的数目随着以后每一次部分或完整的播放录象节目而递减。这些信用单位可与传输的第一密钥一起在报文中下载。

在一个实施例中，这些信用单位是与录象节目的特定段关联的，使得播放录象节目的一段，例如录象节目的第一或最后一刻钟，将减少与这些段关联的一定信用单位。作为替代，信用单位具有单一类型，并随着录象节目的任何段的播放而递减。

如上所述，本发明特别适用于第二密钥算法存储在与记录介质关联的智能卡上的情况。然而，在另一个实施例中，便携式支持是由录象节目本身定义的，第二密钥存储在嵌入数字记录介质外壳中的集成电路中。

这一技术已在诸如 DVHS 盒式录象带的情况中建议，其中可在盒式带外壳的外表面上设置一组金属触点，这些触点导向电子电路，诸如外壳内部的集成电路式芯片。这些触点可与录象机的接受槽中的对应触点组接触，以便能在集成电路与录象机之间通信。

在这些系统中，尽管密钥是用录象节目携带的这一事实，仍提供安全性，因为密钥不能容易地从嵌入芯片内复制。上面对于智能卡实施例

描述的变型同样适用于用录象带外壳定义的支持的系统。

本发明特别适用于扰频数据表示在扰频电视广播中传输的音象数据的方法。

上面已对方法描述了本发明，但同样适用于装置。

为了语言简洁性的目的，这里使用了名词“扰频”与“加密”及“控制字”与“密钥”。然而，应理解在“扰频数据”与“加密数据”之间或“控制字”与“密钥”之间无根本区别。类似地，虽然描述指称“接收机/解码器”及“解码器”，应理解本发明同样适用于具有与解码器集成的接收机及与物理上分开的接收机结合工作的解码器的实施例。本发明同样扩展到解码器与诸如电视或甚至数字录象机等其它设备集成的实施例。

现在相对于附图用只是示例的方式描述本发明的较佳实施例，附图中：

图1示出可用本发明适应成与数字录象设备交互作用数字电视系统的总体结构；

图2示出图1的电视系统的条件访问系统；

图3示出电视系统中的不同加密级；

图4示出电视系统中包含图像、声音、电传正文数据及ECM报文分量的传输的数字分组的结构；

图5示出包含数字录象设备及具有用于加密要登记在数字盒式录象带上的码字的第二算法的智能卡的本发明的第一实施例；

图6示出本发明的第二实施例，其中该智能卡包含分别用于观看传输的与录制的节目所必需的第一与第二密钥两者连同用于确定节目可观看的次数的信用单位；以及

图7示出本发明的第三实施例，其中第二密钥存储在安装在数字盒式录象带的外壳中的集成电路中。

数字电视系统

图1中示出适用于本发明的数字电视广播与接收系统1000的概貌。该系统包含采用已知的MPEG－2压缩系统来传输压缩的数字信号的最常规的数字电视系统2000。更详细地，广播中心中的MPEG－2压缩器2002接收数字信号流（通常是视频信号流）。压缩器2002用链路2006连接在多路复用器与扰频器2004上。多路复用器2004接收多个

其它输入信号，组装一或多个传送流并通过链路 2010 将压缩的数字信号传输给广播中心的发射机 2008，链路 2010 当然可采用包含电信链路在内的各种各样的形式。发射机 2008 通过上行链路 2012 向卫星转发器 2014 发射电磁信号，在那里它们被电子地处理及通过象征性下行链路 2016 广播到地面接收机 2018，后者常规地以最终用户拥有或租用的碟的形式。将接收机 2018 接收的信号传输给最终用户拥有或租用的并连接在该最终用户的电视机 2022 上的集成的接收机/解码器 2020。接收机/解码器 2020 将压缩的 MPEG－2 信号解码成用于电视机 2022 的电视信号。

条件访问系统 3000 连接在多路复用器 2004 与接收机/解码器 2020 上并部分地位于广播中心及部分地位于解码器中。它使最终用户能访问来自一或多个广播供应商的数字电视广播。可将能解密关于商品出售的消息（即关于广播供应商出售的一或多个电视节目）的智能卡插入接收机/解码器 2020。利用解码器 2020 与智能卡，最终用户可用订阅方式或每看一次付费的方式购买项目。

也连接在多路复用器 2004 与接收机/解码器 2020 上并且又是部分地位于广播中心及部分地位于解码器中的交互系统 4000 使用户能通过调制解调的返回频道 4002 与各种应用交互作用。

条件访问系统

参见图 2，条件访问系统 3000 包括用户授权系统（SAS）3002。SAS3002 用各自的 TCP－IP 链路 3006（虽然其它类型的链路也可代替使用）连接在一或多个用户管理系统（SMS）3004 上，每一个广播供应商一个。作为替代，两个广播供应商可共用一个 SMS，或一个供应商可用两个 SMS，等等。

以利用“母”智能卡 3010 的密码单元 3008 的形式的第一加密单元用链路 3012 连接在 SAS 上。又是以利用母智能卡 3016 的密码单元 3014 的形式的第二加密单元用链路 3018 连接在多路复用器 2004 上。接收机/解码器 2002 接纳“女儿”智能卡 3020。它通过调制解调的返回频道 4002 用通信服务器 3022 直接连接在 SAS3002 上。SAS 发送订阅权利及其它事物给请求中的女儿智能卡。

智能卡包含一或多个商业经营者的机密。“母”智能卡加密不同种类的报文而“女儿”智能卡解密这些报文，如果她们有权这样做的话。

第一与第二密码单元 3008 与 3014 包括支架、带有存储在 EEPROM 上的软件的电子 VME 卡、分别多达 20 个电子卡及一个智能卡 3010 与 3016，对于各电子卡，一张（卡 3016）用于加密 ECM 及一张（卡 3010）用于加密 EMMS。

如下面描述的，ECM 即权利控制报文是嵌入传输的节目的数据流中的加密报文并包含解密节目所必需的控制字。给定的接收机/解码器的授权受在较不频繁的基础上传输（例如每月一次）的 EMM 即权利管理报文的控制，并且 EMM 提供给授权的接收机/解码器解码 ECM 所必需的密钥。

下面参照电视系统 2000 与条件访问系统 3000 的各部件更详细地描述数字电视系统的条件访问系统 3000 的操作。

多路复用器及扰频器

参见图 1 与 2，在广播中心，首先使用 MPEG－2 压缩器 2002 压缩（或降低位率）数字视频信号。然后通过链路 2006 将这一压缩信号传输到多器复用器与扰频器 2004 以便与诸如其它压缩数据等其它数据多路传输。

扰频器生成在扰频过程中使用的控制字 Ce 并在多路复用器 2004 中将其包含在 MPEG－2 流中。控制字 Ce 是内部生成的并使最终用户的集成接收机/解码器 2020 能解扰节目。指明如何将节目商品化的访问标准也加入到 MPEG－2 流中。可用若干种“订阅”方式之一与/或若干种“每观看一次付费”（PPV）方式或事件之一商品化节目，在订阅方式中，最终用户订购一或多个“花束”的商品供应，从而得到观看这些花束内每个频道的观看权。在较佳实施例中，可从频道花束中选择多达 960 种商品供应。在每观看一次付费方式中，向最终用户提供根据他的意愿购买项目的能力。这能通过事先预订项目（“预订方式”）或通过一广播立即购买项目（“冲动方式”）来达到。

使用控制字 Ce 与访问标准两者来建立权利控制报文（ECM）；这是与一个扰频节目相关发送的报文；这一报文内含控制字（它允许解扰该节目）与该广播节目的访问标准。通过链路 3018 将访问标准与控制字传输到第二加密单元 3014。在这一单元中生成 ECM，用第一密钥 Cex 加密并向前传输到多路复用器与扰频器 2004。

广播供应商的各服务广播在数据中包括若干不同的分量；例如电视

节目包括视频分量 V、音频分量 S、子标题或电传正文分量 T 等等（见图 4）。服务的这些分量中的各个是单独扰频与加密供随后广播到转发器 2014 上的。关于服务的各扰频分量，需要分开的 ECM。

节目传输

多路复用器 2004 接收包括来自 SAS3002 的加密 EMM、来自第二加密单元 3014 的加密 ECM 及来自压缩器 2002 的压缩的节目的电信号。多路复用器 2004 扰频节目并通过链路 2010 将扰频的节目、加密的 EMM(如果存在的话）与加密的 ECM 作为电信号传输给广播中心的发射机 2008。发射机 2008 通过上行链路 2012 发射电磁信号到卫星转发器 2014。

节目接收

卫星转发器 2014 接收及处理发射机 2008 发射的电磁信号并通过下行链路 2016 将信号继续发射到常规上以最终用户拥有或租用的碟的形式的地面接收器 2018。将接收器 2018 接收的信号传输到最终用户拥有或租用的并连接在该最终用户的电视机 2022 上的集成的接收机/解码器 2020。接收机/解码器 2020 多路分解该信号以获得带有加密的 EMM 与加密的 ECM 的扰频的节目。

如果节目不是扰频的，则接收机/解码器 2020 解压数据并将信号变换成视频信号供传输给电视机 2022。

如果节目是扰频的，则接收机/解码器 2020 从 MPEG－2 流中抽取对应的 ECM 并将该 ECM 传递给最终用户的“女儿”智能卡 3020。这插入接收机/解码器 2020 中的外壳中。女儿智能卡 3020 控制最终用户是否有权解密 ECM 及访问节目。

如果用户没有必要的权利，便将负面状态传递给接收机/解码器 2020 表示节目不能解扰。如果最终用户有权，则解密 ECM 并抽取控制字。然后解码器 2020 便能用控制字解扰节目。将 MPEG－2 流解压与翻译成视频信号向前传输给电视机 2022。

下面相对于图 3 更详细地描述使用的加密级。

用户管理系统（SMS）

用户管理系统（SMS）包含管理所有最终用户文件、商品节目供应（诸如价目表与促销）、预订、PPV 细节、关于最终用户消费与授权以及其它事物的数据库 3024。SMS 可实际上远离 SAS。

每个 SMS3004 通过各自的链路 3006 发送报文给 SAS3002 使之能修

正或建立要传输给最终用户的权利管理报文（EMM）。

SMS3004 还发送报文给 SAS3002，这些报文隐含不修改或建立 EMM 而只蕴含最终用户的状态改变（在订购产品时关于授于最终用户的权限或关于最终用户将付的费用）。

权利管理报文（EMM）

EMMO 为专用于单个最终用户或一组最终用户的报文（与 ECM 不同，它只用于一个扰频节目或作为同一商品节目供应的部分的一组扰频节目）。一组可包括给定数目的最终用户。作为一组的这种组织形式的目标在于优化带宽，即，对一组的访问能允许到达大量最终用户。

在实行本发明中使用了各种特定类型的 EMM。个人 EMM 专用于个人用户，并且通常用在提供每观看一次付费的服务；它们包含组标识符及用户在该组中的地位。所谓的“组”订阅 EMM 专用于诸如 256 个个人用户的组，并且通常用于某些订阅服务的管理。这一 EMM 具有组标识符及用户的组位图。观众 EMM 专用于全体观众，并可诸如由特定经营者用来提供某些免费服务。“观众”是具有载有同一经营者标识符（OPI）的智能卡的全体用户。最后，将“唯一”的 EMM 给于智能卡的唯一标识符。

系统的加密级

参见图 3，现在描述广播系统中的加密级。与数字数据的广播关联的加密级示出在 4001 上，传输频道（诸如上述卫星链路）示出在 4002 上，而接收机上的解密级示出在 4003 上。

在传输给多路复用器 Mp 供接着传输之前，用控制字 Ce 扰频数字数据 N。从图 4 中可见，传输的数据包含 ECM，后者除别的以外包含受第一加密密钥 Cex 控制的加密器 Ch1 加密的控制字 Ce。在接收机/解码器上，信号在被传递给电视机 2022 供观看之前通过多路分解器 DMp 与解扰器 D。解密单元 Dch1 还拥有解密多路分解的信号中的 ECM 来获取随后用于解扰该信号的控制字 Ce 的密钥 Cex。

为了安全起见，嵌入加密的 ECM 中的控制字平均每 10 秒左右改变一次。反之，接收机用来解码 ECM 的第一加密密钥 Cex 每月左右用 EMM 改变一次。加密密钥 Cex 是由第二单元 ChP 用对应于解码器本体的个人化密钥 Cg 加密的。如果该解码器是选择来接收更新的密钥 Cex 的解码器之一，则该解码器中的解密单元 DChP 将利用其密钥 Cg 来解密报文以获取该月的密钥 Cex。

解密单元DChp与DCh1及相关密钥是保持在提供给用户并插入解码器中的智能卡阅读器中的智能卡上的。这些密钥可按照诸如DES等任何已知的对称密钥算法生成。采用公开/秘密密钥算法的其它实施例也同样可能。

数字数据的录制

如在引言中提出的，有鉴于产生未经授权的复制与盗版的危险性，不建议允许录制解扰的数字数据。如图5中所示，本发明提供了克服这一问题的装置。

该系统包括可插入接收机/解码器中的智能卡槽中的智能卡 4004以及包含诸如DVHS盒式带等数字记录介质4006的DVHS录象机等数字录象机4005。

在本实施例中，由插入解码器（见图 2）的相关智能卡 3020解密所接收的控制字。然后将解码的控制字 Ce（连同构成 ECM 的任何其它数据，诸如访问控制信息等）传递给嵌入该智能卡4004中的微处理器。智能卡 4004利用第二加密密钥 C2及第二加密算法 Ch2生成新的ECM，在图中表示为ECM'。然后用权利报文ECM'替换来自多路分解器DMp的扰频数据流中的 ECM，如 4007 上所示，并将扰频数据与新的权利报文ECM'的组合录制在DVHS盒式带4006上。可将权利报文ECM'插入在移位控制寄存器R中流通的数据流中。

用这一方法，本发明避免在盒式带上录制解码的音象信息。为了播放盒式带，将卡重新插入解码器中，利用密钥C2解码权利报文ECM'及随后抽取的用于控制解码器解扰节目供观看的控制字Ce。

在图5中所示的系统中，智能卡4004是与电视系统的图2中所示的包含观看节目所必需加密密钥的智能卡 3020不同的。然而，在图6中所示的另一实施例中，智能卡 3020包含观看与录制节目所需要的第一与第二加密密钥Cex与C2两者。如所示，密钥Cex控制ECM的解密来生成解码器D用来观看节目的控制字Ce及随后用密钥C2加密以构成新的权利报文ECM'。

为了节省空间未示出算法DCh1与DCh2。实际上卡3020也通常用能解密EMM以便能获得存储在该卡的存储器中的当月的密钥Cex的个人化密钥Cg（未示出）初始化。虽然以基本上矩形卡的形式示出智能卡，当然诸如钥匙形等其它物理形式也是可能的。

与节目一起传输并用卡解密的ECM也可包括随后存储在卡中的信用单位U，它们控制可观看录制的影片的次数。在最简单的实施例中，信用单位可在每一次解码器传递ECM'时重新播放录制的影片时递减，一旦信用数已递减到零，表示录制的节目已观看了预定的次数，便将一报文发送给解码器以防止再观看该影片，除非重新支付信用单位（例如通过在EMM中发送收费指令）。

在另一实施例中，信用单位可可每10个或100个ECM'报文递减一次。在又另一实现中，信用单位可对应于影片的某些部分（例如影片的最前面或最后10分钟），使得播放这些部分递减与之相关的信用单位。这些部分可通过相应地标记这些部分中的ECM'报文来标识。

图7中示出本发明的又一实施例。在这一实施例中，新的权利报文EMM'的生成是受拥有第二加密密钥C2并嵌入录制的盒式带4006的外壳中的集成电路或芯片4008控制的。在记录介质的外壳内加入微处理器是已知技术并已在诸如DVHS盒式带的情况中建议。在本例中，可在盒式带外壳的外表面上设置一组金属触点，这些触点引导到电子电路，诸如外壳内部的集成电路或芯片。这些触点可用录象机的接受插槽中的对应触点组压紧以便能在集成电路与录象机之间通信。

如将理解的，虽然复制记录（与扰频）的数字数据是简单的，存储在芯片中的数据将抵制复制，并且如在前面的实施例中，没有解锁ECM'来获取解扰器所用的控制字所必需的密钥C2，扰频的数据将是毫无用处的。

如会理解的，在上述所有实施例中，接收机/解码器与数字记录设备的元件可以组合或互换，例如使得数字录象机拥有用于接纳智能卡的智能卡槽，与/或一旦从ECM'报文中抽取了控制字Ce时解扰节目所必需的文件。解码器与/或数字录象机也同样能与诸如电视机等其它设备集成在一起。

00-05-25

说 明 书 附 图

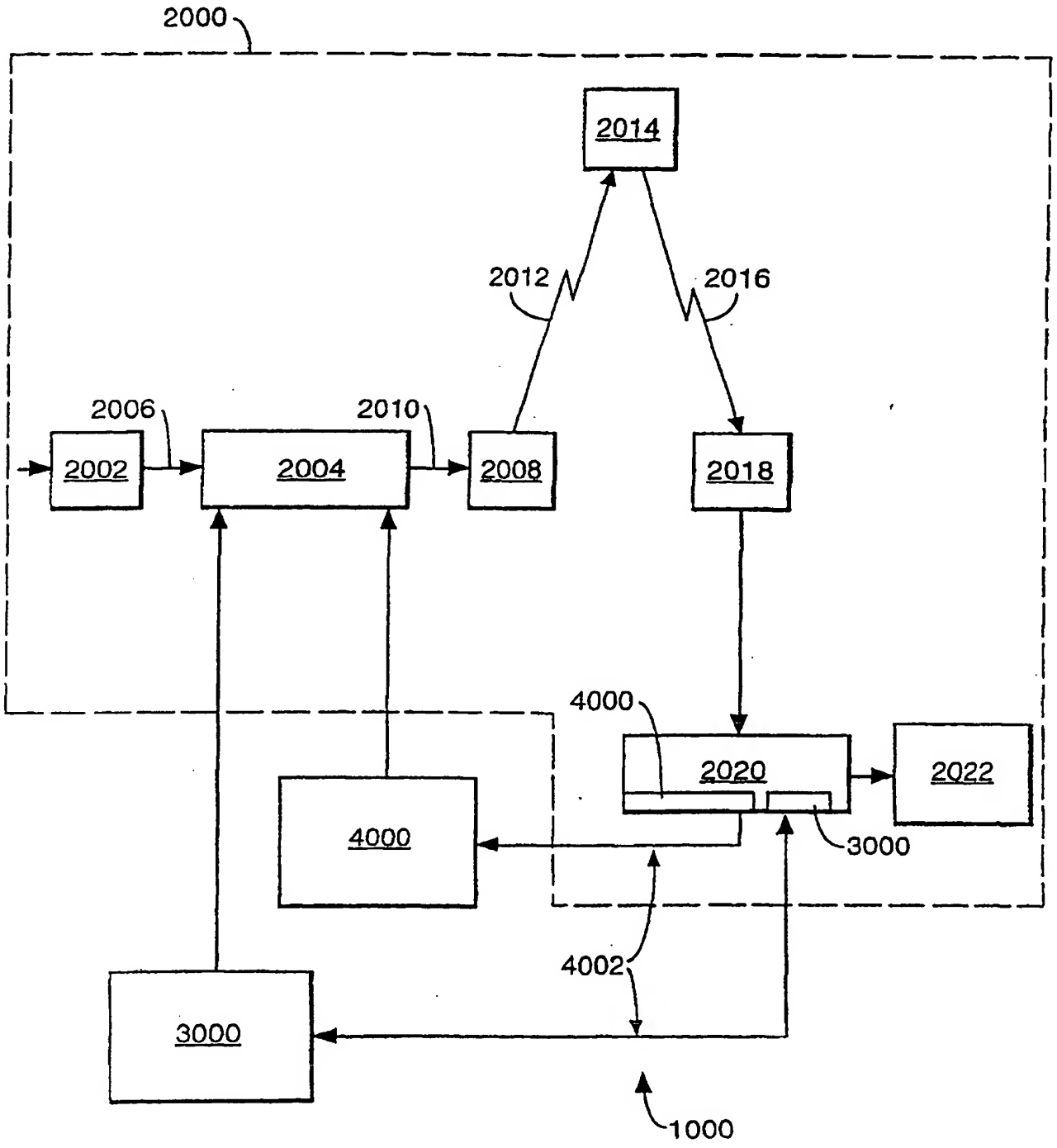


图 1

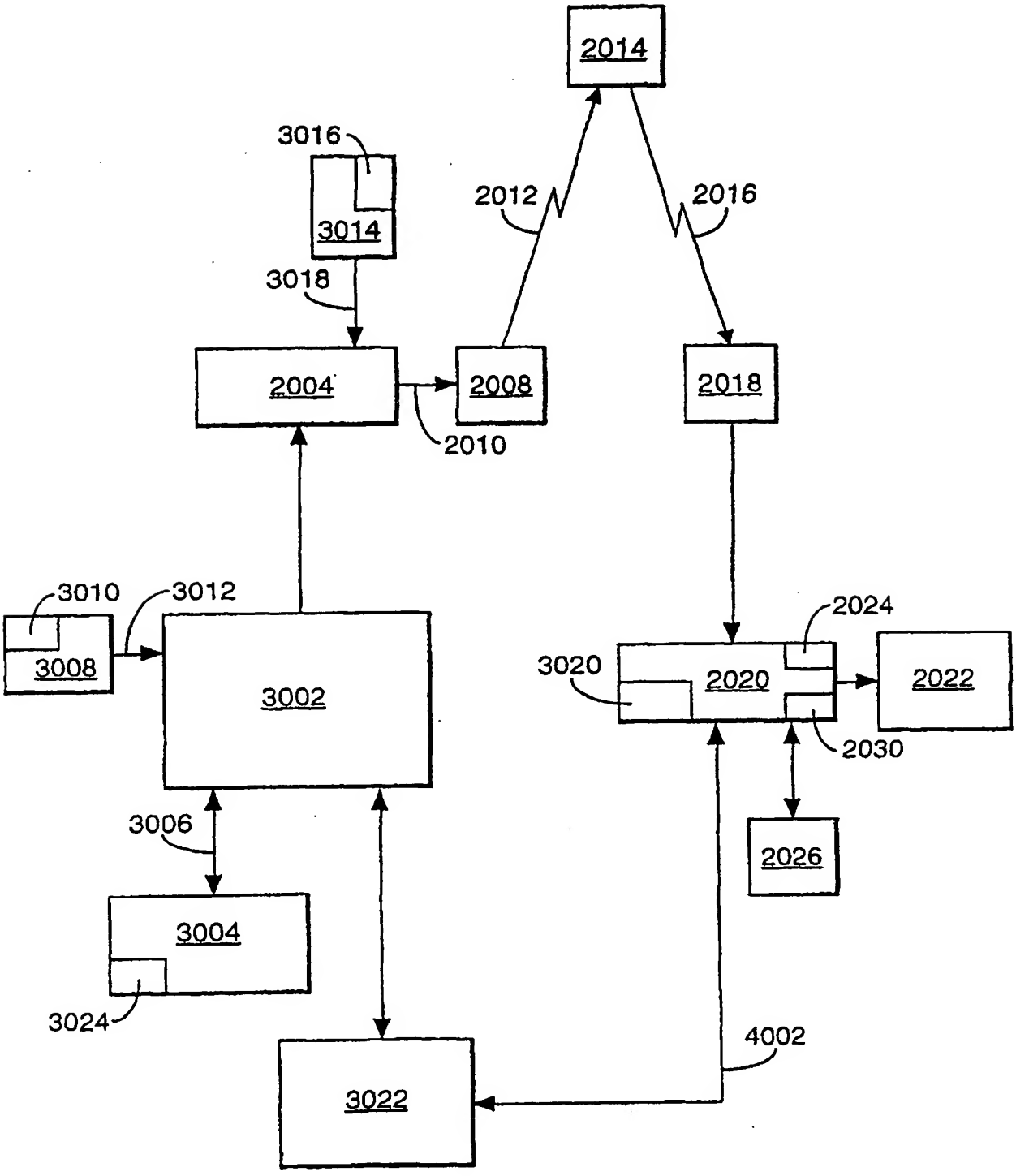

2014
3016
3014
2012
2016
3018
2004
2008
2018
2010
3010
3012
3008
3002
2024
3020
2020
2022
2030
3006
2026
3004
3024
4002
3022

图 2

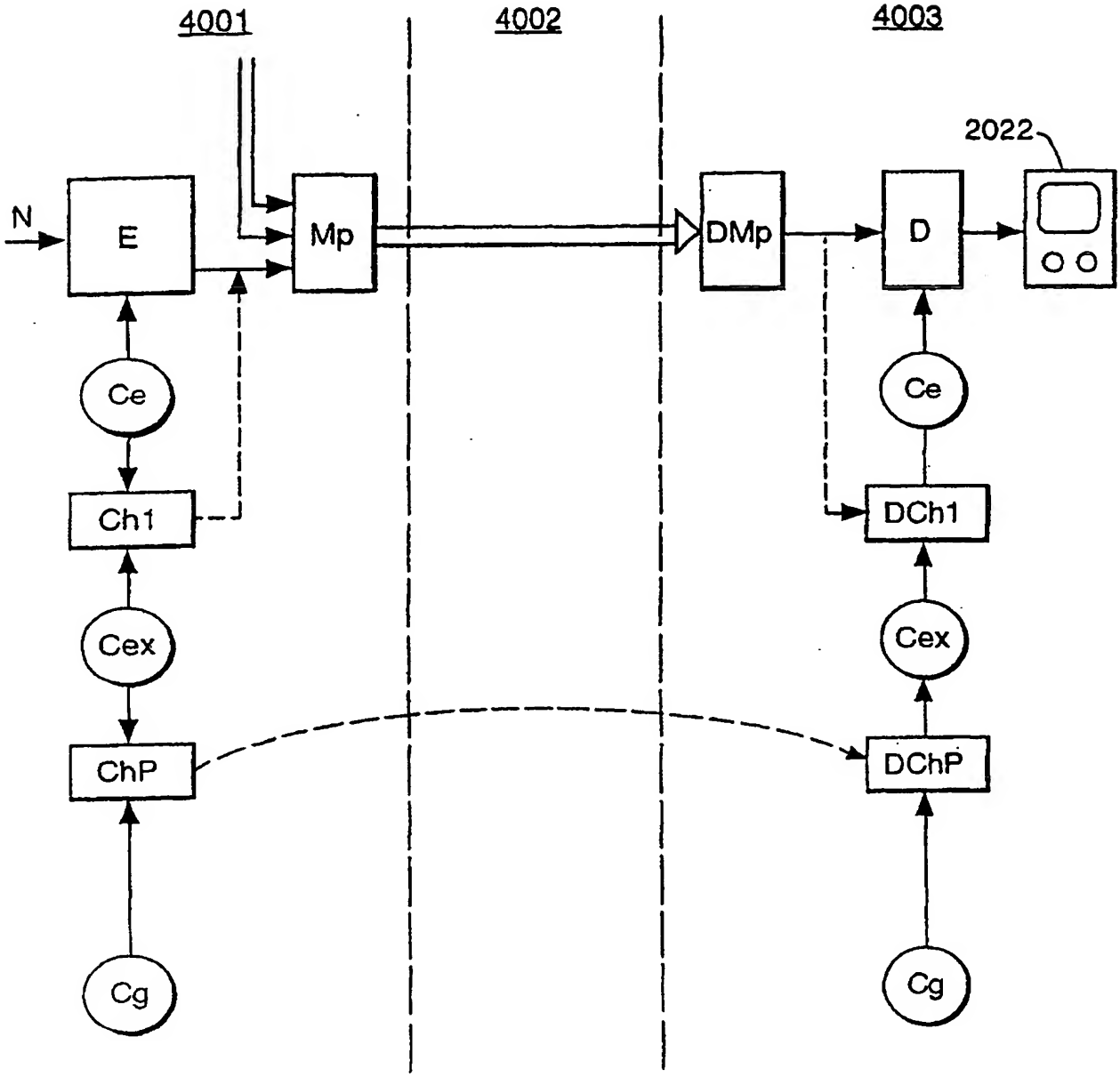

4001
4002
4003
2022
N
E
Mp
DMp
D
Ce
Ch1
Cex
ChP
Cg
Ce
DCh1
Cex
DChP
Cg

图 3

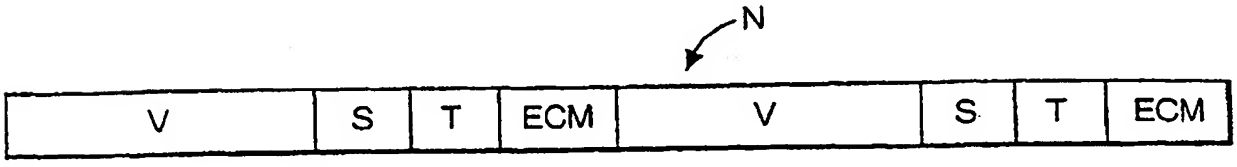

N
V
S
T
ECM
V
S
T
ECM

图 4

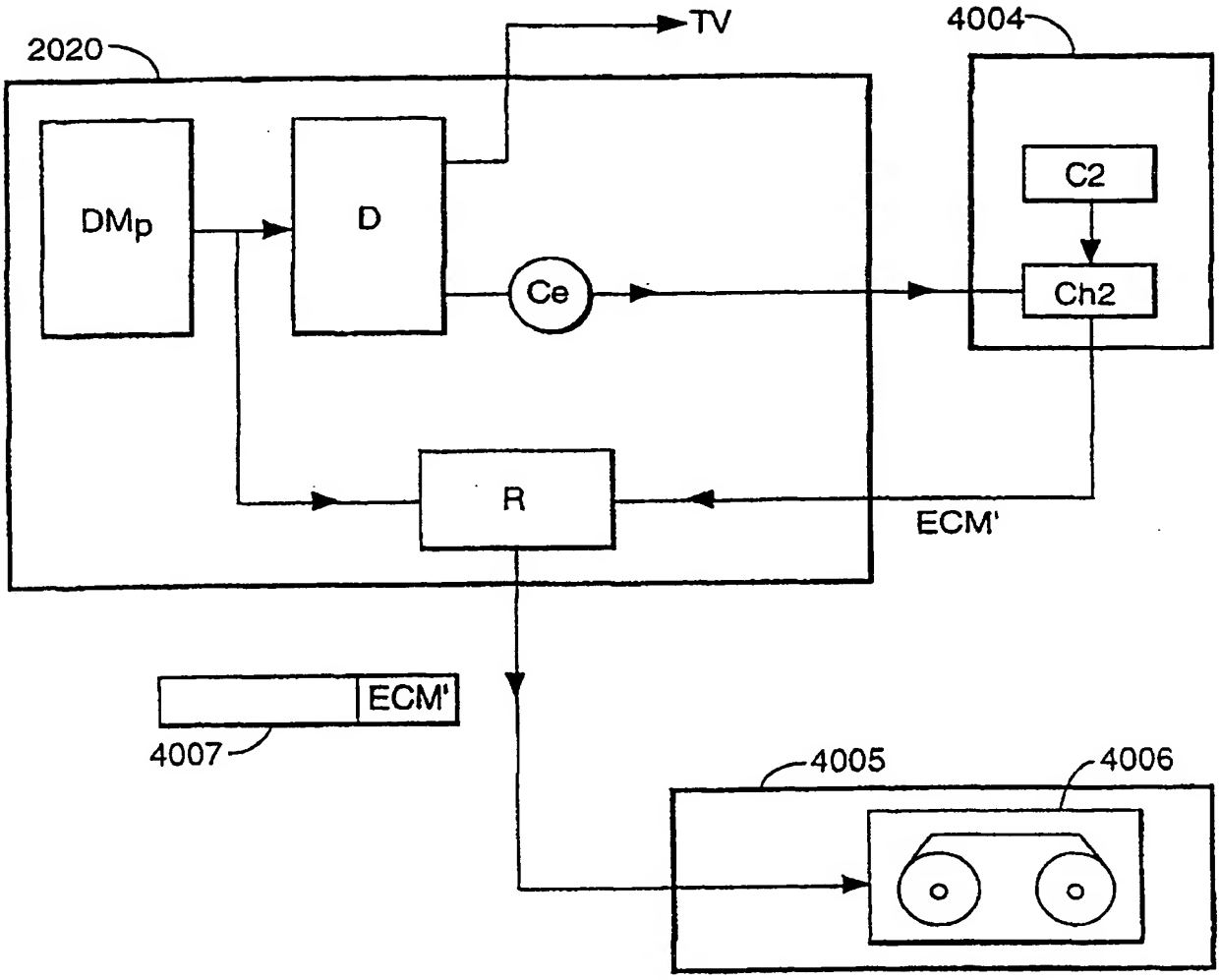


图 5

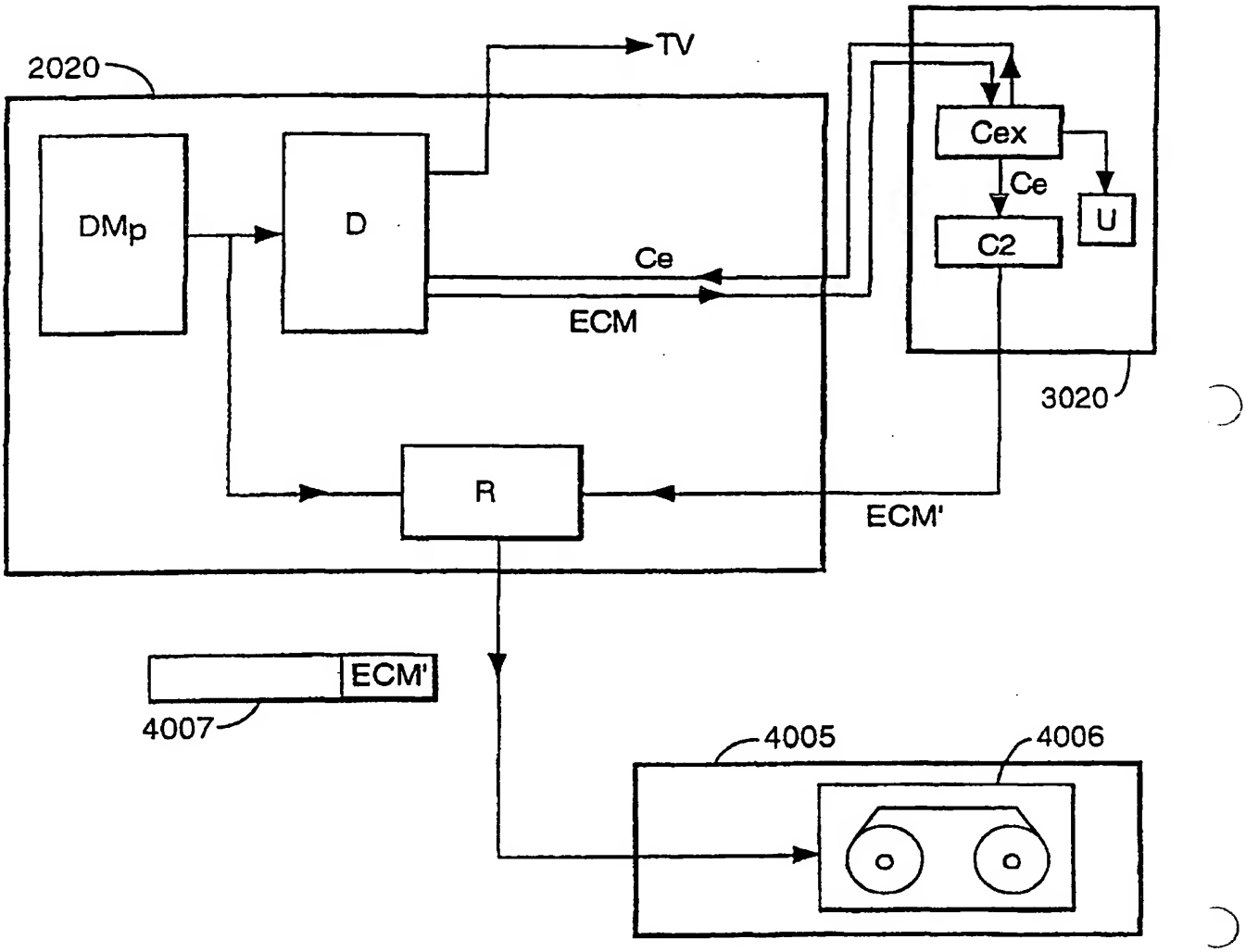


图 6

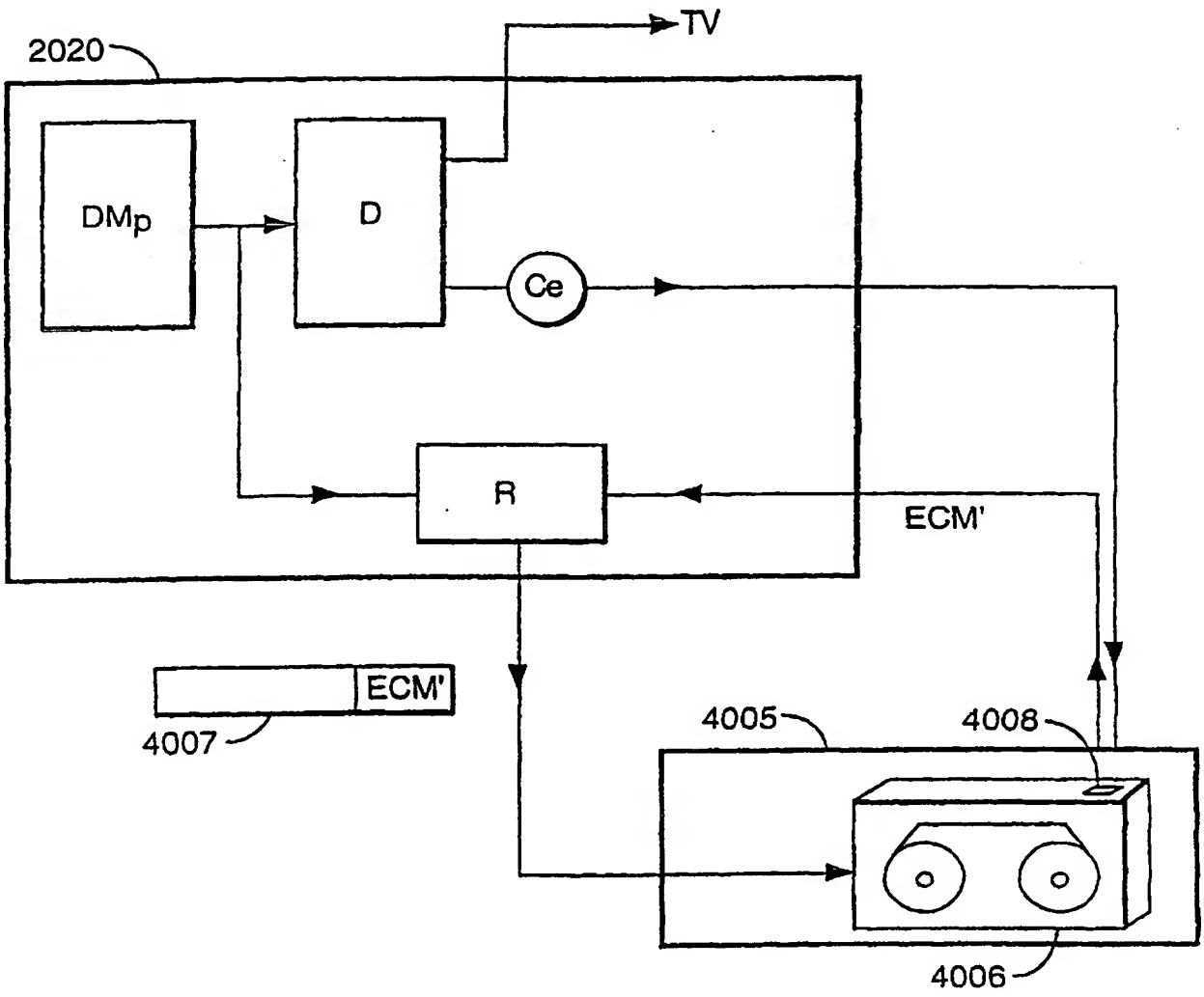


图 7